Comment vaincre le chiffre de VIGENERE ?

Le système de chiffrement de VIGENERE résista durant trois siècles jusqu'à ce que le mathématicien Charles BABBAGE élabore la théorie de son décodage.

L'essentiel : Trouver la longueur de la clè
Reprenons le message proposé lors de la deuxième séance :

BYCOT RSONP NIFUP DOVFD WOTTJ APHLG RUGMC QOQWF LCOGN FEZUE TJEWS
EUUEI BLCVX FFUZB NIMEU JNVFR KFUTT EVPPR PSGTE VMEUU RQJSC OGNFS
KOTGS IGVRU TOPUE IBUZB DGVXF SOKUS GVCNJ DGQRQ QOUJT KPNZY XKJ

Si la longueur de la clé est 5, alors les 1ère, 6ème, 11ème …..... lettres ont toutes été codées selon le même principe : **un décalage de César.** Une analyse des fréquences de cette série de lettres permet alors de retrouver le décalage et de retrouver le message en clair. On procède alors de même avec les 2ème , 7ème, 12ème …. lettres et ainsi de suite .

Dans le message codée ci-dessous, la clé est de longueur 5. Décoder ce message .
RSGAM ACJHT WSWNX ASGKI BWVKE XBKKS SIZKI ASJLC HHVFI

HRVVS DFUHR CSVLI CUVHQ THIBI DBCNM SCZME JGJBP TGCHM

HRVEE GSWKE RHZHR TBFIX XELXE XBJBU JIEXV TTCXB XCELY

GZFKM VWEXH JGPLX TAVLS AOZKI

Et si on ne connaît pas la longueur de la clé ?

On utilise alors **l'indice de coïncidence.** Inventé, vers 1920, par William Friedman, cet indice (IC) correspond à la probabilité que deux lettres choisies au hasard dans un texte soient identiques .

Par exemple, dans un texte composé de 100 lettres et contenant 12 fois la lettre A, si on tire deux lettres au hasard, on a 12 chances sur 100 d'obtenir un A au premier tirage et 11 chances sur 99 d'obtenir à nouveau un A au deuxième tirage. La probabilité de tirer deux A est donc $\frac{12}{100} \times \frac{11}{99}$

Pour obtenir l'indice de coïncidence de ce texte complet, on procède alors de même avec les autres lettres et on ajoute les 26 probabilités ainsi obtenues.

Calculer l'indice de coïncidence du texte précédent : IC =

Comment utiliser ce principe pour décoder VIGENERE ?

On sait qu'en langue française, cette probabilité est proche de 0,074.
Dans le texte précédent, vous devez avoir trouvé un IC trop éloigné de 0,074. La longueur de la clé ne doit pas être 1.
On calcule alors l'IC en ne considérant qu'une lettre sur deux puis une lettre sur trois etc....
L'IC qui se rapproche le plus de 0,074 permet de donner la longueur de la clé.

L'algorithme suivant permet de calculer les IC en supposant une longueur de clé inférieure ou égale à 7.
Reproduire cet algorithme sur Algobox et chercher à percer le mystère du message proposé en début de séance

BYCOT RSONP NIFUP DOVFD WOTTJ APHLG RUGMC QOQWF

LCOGN FEZUE TJEWS EUUEI BLCVX FFUZB NIMEU JNVFR

KFUTT EVPPR PSGTE VMEUU RQJSC OGNFS KOTGS IGVRU

TOPUE IBUZB DGVXF SOKUS GVCNJ DGQRQ QOUJT KPNZY XKJ

Présentation de l'algorithme

Calculer l'indice de coincidence dans un texte crypté
Texte à rentrer en MAJUSCULE SANS ESPACE longueur de clé maximum 7

```
VARIABLES
    decode EST_DU_TYPE CHAINE
    a EST_DU_TYPE LISTE
    i EST_DU_TYPE NOMBRE
    b EST_DU_TYPE LISTE
    j EST_DU_TYPE NOMBRE
    Ic EST_DU_TYPE NOMBRE
    k EST_DU_TYPE NOMBRE
    l EST_DU_TYPE NOMBRE
    m EST_DU_TYPE NOMBRE
    tampon EST_DU_TYPE CHAINE
    N EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
    LIRE decode
    POUR i ALLANT_DE 1 A 7
        DEBUT_POUR
        tampon PREND_LA_VALEUR ""
        Ic PREND_LA_VALEUR 0
        POUR l ALLANT_DE 1 A tampon.length
            DEBUT_POUR
            a[l] PREND_LA_VALEUR 0
            FIN_POUR
        k PREND_LA_VALEUR 0
        TANT_QUE (k<=decode.length) FAIRE
            DEBUT_TANT_QUE
            tampon PREND_LA_VALEUR tampon+decode.substr(k,1)
            k PREND_LA_VALEUR k+i
            FIN_TANT_QUE
        POUR j ALLANT_DE 1 A tampon.length
            DEBUT_POUR
            a[j] PREND_LA_VALEUR tampon.charCodeAt(j-1)
            FIN_POUR
        POUR j ALLANT_DE 65 A 90
            DEBUT_POUR
            N PREND_LA_VALEUR 0
            POUR m ALLANT_DE 1 A tampon.length
                DEBUT_POUR
                SI (a[m]==j) ALORS
                    DEBUT_SI
                    N PREND_LA_VALEUR N+1
                    FIN_SI
                FIN_POUR
            Ic PREND_LA_VALEUR Ic+N*(N-1)/(tampon.length*(tampon.length-1))
            FIN_POUR
        AFFICHER "indice intervalle "
        AFFICHER i
        AFFICHER Ic
        FIN_POUR
    FIN_ALGORITHME
```